FortiNAC

L2 and L3 Network Types

Version: 8.x

Date: January 28, 2020

Rev: A

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

http://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

http://www.fortinet.com/support-and-trainingt/training.html

NSE INSTITUTE

http://training.fortinet.com

FORTIGUARD CENTER

http://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

F⊡RTINET

Monday, September 10, 2018

Contents

Overview

This document explains the Network Types available when configuring FortiNAC. For more information on appliance configuration, see the appropriate installation guide in the Fortinet Document Library.

There are two network type options:

- **Layer 2 network**: Isolation networks are switched to the FortiNAC eth1 interface. 802.1Q tags are configured for the corresponding isolation VLANs, and eth1 IP addresses are within those isolation networks. See Layer 2 for illustrations

- **Layer 3 network**: Isolation networks are routed to the FortiNAC eth1 interface.   See Layer 3 for illustrations

  Important: In a High Availability environment with L3 configuration (redundant FortiNAC servers on different subnets and do not use a shared IP address), the Layer 3 network option is required. L3 High Availability configurations are not supported with Layer 2 Isolation settings.
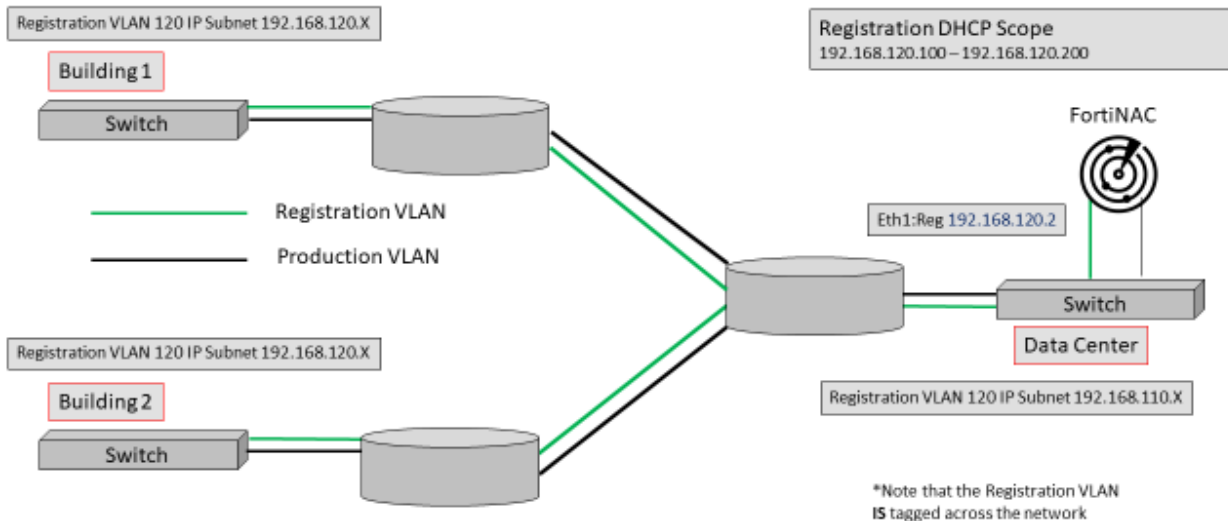
Layer 2

Layer 2 Implementation

- The isolation interface
  - 802.1q trunk
  - The interface accepts traffic tagged from any of the isolation VLANs
  - Same broadcast domain as hosts
  - IP address for each isolation subnet

Eth 1

DeadEnd – 192.168.112.2   VLAN 112
Quarantine – 192.168.111.2   VLAN 111
Registration – 192.168.110.2   VLAN 110
VLAN 115

Layer 2 "Flat" Deployment

Registration VLAN 120 IP Subnet 192.168.120.X

Building 1

Switch

Registration DHCP Scope
192.168.120.100 – 192.168.120.200

FortiNAC

—— Registration VLAN

—— Production VLAN

Eth1:Reg 192.168.120.2

Switch

Data Center

Registration VLAN 120 IP Subnet 192.168.120.X

Building 2

Switch

Registration VLAN 120 IP Subnet 192.168.110.X

*Note that the Registration VLAN
IS tagged across the network
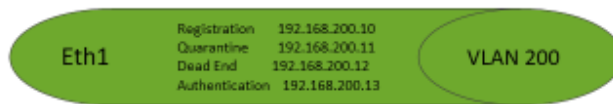
Layer 3

Layer 3 Implementation

- The isolation interface is a standard interface
  - The interface exists on a single network
  - The interface is not within the same broadcast domain as a host assigned to an isolation network
  - The interface uses multiple IP addresses within the same subnet
  - DHCP relays must be configured on each isolation network pointing back to the isolation interface
  - The individual IP address are used by DNS

Eth1	Registration	192.168.200.10	VLAN 200
	Quarantine	192.168.200.11	
	Dead End	192.168.200.12	
	Authentication	192.168.200.13	

Layer 3 "Routed" Deployment

Registration VLAN 200 (Bldg 1 Reg)
Relay Address = 192.168.200.10

Registration = 192.168.200.10
Registration DHCP Scopes =   Bldg 1 Reg
                             Bldg 2 Reg

Building 1

Switch

DHCP Relay for
Registration VLAN

FortiNAC

Eth1 on 192.168.200.0

—— Registration VLANs

—— Production VLAN

Registration VLAN 300 (Bldg 2 Reg)
Relay Address = 192.168.200.10

Switch

Data Center

Building 2

Switch

DHCP Relay for
Registration VLAN

DHCP Relay for
Registration VLAN

FNAC Stub VLAN 100 ——
Relay Address = 192.168.200.10